REMARKS / DISCUSSION OF ISSUES

Claims 1-10 are pending in the application. Claims 9 and 10 are newly added.

The applicant thanks the Examiner for acknowledging the claim for priority and receipt of certified copies of all the priority documents.

The applicant thanks the Examiner for noting that the drawings are acceptable.

Claims are amended for non-statutory reasons: to correct one or more informalities, remove figure label numbers, and/or to replace European-style claim phraseology with American-style claim language. The claims are not narrowed in scope and no new matter is added.

The Office action objects to the annotation "(pseudo-)" before "randomly" in claims 1, and "random" in claim 5. The annotation is deleted herein, so as to use the broader, non-annotated adverb and adjective. The applicant respectfully notes that the term "random" process is generally known to include automated means for producing "random" variables, and such automated means are generally termed "pseudo-random", because they typically produce random variables in a repeatable manner (i.e. given the same seed and generator, the same sequence of random variables will be produced; however, absent knowledge of the seed, the variables are effectively random).

The Office action rejects claims 1, 3-4, and 7-8 under 35 U.S.C. 103(a) over Rijmen et al. ("The Cipher SHARK", hereinafter Rijmen), and Loureiro et al. ("Function Hiding Based on Error Correcting Codes", hereinafter Loureiro). The applicant respectfully traverses this rejection.

The applicant respectfully maintains that there is no suggestion in the prior art to combine Rijmen and Loureiro, and that even if Rijmen and Loureiro are combined, they do not provide the applicant's claimed invention.

Claim 1, upon which each of the other rejected claims depends, claims a method of generating a linear transformation matrix A for use in a symmetric-key cipher, that includes generating a binary [n,k,d] error-correcting code, using a generator matrix $G = (I_k \| B)$, with $B \in Z_2^{k\times(n-k)}$, where $k < n < 2k$, and extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving matrix A from matrix C.

Rijmen teaches a symmetric-key cipher, but does not teach generating a binary error-correcting code using a generator matrix $G = (I_k \| B)$, with $B \in Z_2^{k\times(n-k)}$, where $k < n < 2k$. At page 5, line 2, Rijmen specifically teaches a generator matrix $G = (I_n \| B)$, with $B \in Z_2^{n\times n}$. Rijmen presents this generator matrix as a significant improvement over conventional MDS codes, and does not suggest using a different generator matrix.

Loureiro teaches a method of "hiding functions instead of encrypting data vectors" (Loureiro's abstract). Referring to FIG. 1: a user encrypts a function f using an encrypter E, and provides the encrypted function E(f) to another user, for use in its encrypted form. When given an input x, the encrypted function E(f) provides a result y' that can be decrypted D to determine the result y that would have been produced by un-encrypted function f(x). To create an encrypter that provides an encrypted function whose output can be decrypted to find the proper result, an error-correcting-code cryptosystem is used.

Loureiro's system is unrelated to a symmetric-key cipher such as taught by Rijmen for encrypting data vectors. Loureiro presents his system as an alternative to encrypting data vectors. Because Rijmen and Loureiro each teach a substantially different approach to encryption, with Rijmen teaching the encryption of data vectors, and Loureiro teaching the encryption of operable functions, one of ordinary skill in the art would not be lead to combine these teachings.

The Office action asserts that the motivation to combine the references "would have been to hide a function represented on a matrix format". The applicant fails to find a reference in either Rijmen or Loureiro for this asserted motivation, and respectfully maintains that merely having a motivation to hide a function represented on a matrix format would not lead one to combine Rijmen or Loureiro, because Loureiro does not, per se, address functions represented on a matrix format.

Assuming in argument that one of ordinary skill in the art might be lead to combine Rijmen and Loureiro, the applicant respectfully maintains that such a combination would not be suitable for its intended function, and that such a combination would not produce the applicant's claimed invention.

Rijmen teaches a symmetric key cipher for encrypting data that uses a linear transformation function. Loureiro teaches a means for creating an encrypted function that produces an output that can be subsequently decrypted to provide the proper output. If Loureiro's invention is used to encrypt Rijmen's transformation function, to hide the function as the Office action asserts, the applicant respectfully maintains that the resulting output from the encrypted function will not be the proper output from Rijmen's linear transformation function, and will not necessarily have the required characteristics of a linear transformation used for cryptographic purposes. Rijmen recites a number of required characteristics of the codes in the linear transformation matrix, including being invertible, having a high minimum Hamming weight, a high branch number, and so on. There is not evidence in Loureiro that an encrypted function has the same characteristics as the unencrypted function, and, in general, encrypted forms of items are generally designed to have dissimilar characteristics from the original item, to hide such characteristics from detection.

Assuming in argument that a Loureiro-encrypted function of Rijmen's linear transformation function were operable for cryptographic purposes, the combination of Loureiro and Rijmen would not produce the applicant's claimed invention.

The applicant specifically claims extending matrix B with 2k-n columns such that a resulting matrix C is non-singular. Neither Loureiro nor Rijmen teach or suggest extending a matrix with 2k-n columns, and neither Loureiro nor Rijmen teach that such an extension should be configured such that the resulting matrix is non-singular.

The Office action acknowledges that Rijmen does not teach extending matrix B with 2k-n columns, and asserts that Loureiro's section 4.1 provides this teaching. At the referenced section, Loureiro teaches multiplying a kxk matrix (F), an [n, k, d] generator function (G), and an nxn matrix (P) to produce a kxn matrix (FGP) that is added to kxn matrix (E). Nowhere in the cited text does Loureiro teach extending a matrix by 2k-n columns, and nowhere in the

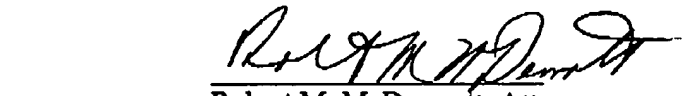
cited text does Loureiro teach extending a matrix such that the resulting matrix is non-singular.

The Office action rejects claims 2 and 5 under 35 U.S.C. 103(a) over Rijmen, Loureiro, and FOLDOC ("brute force"). The applicant respectfully traverses this rejection based on the remarks above regarding claim 1, upon which claims 2 and 5 depend. FOLDOC does not cure the deficiencies of Rijmen and Loureiro with regard to claim 1.

Because neither Rijmen nor Loureiro, individually or collectively, teach or suggest a method of generating a linear transformation matrix A for use in a symmetric-key cipher, that includes generating a binary [n,k,d] error-correcting code, using a generator matrix $G = (I_k \| B)$, with $B \in Z_2^{k\times(n-k)}$, where $k < n < 2k$, and extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving matrix A from matrix C, as specifically claimed by the applicant, the applicant respectfully requests the Examiner's reconsideration of the rejections of claims 1-8 over Rijmen and Loureiro.

In view of the foregoing, the applicant respectfully requests that the Examiner withdraw the rejections of record, allow all the pending claims, and find the application to be in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,



Robert M. McDermott, Attorney
Registration Number 41,508
patents@lawyer.com

1824 Federal Farm Road
Montross, VA 22520
Phone: 804-493-0707
Fax: 215-243-7525